No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**						
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**						
A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y las partes externas pertinentes.	SI	A4.MS.DE Anexo 4 Manual Políticas de Seguridad de la Información.	X		
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	SI	La política de Seguridad de la Información del ICBF deberá ser revisada en intervalos planificados por Dirección (una vez al año).	X		
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**						
A.6.1	**Organización interna**						
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.	SI	Resolución 7070 de 2017.	X	X	X
A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	SI	Resolución 7070 de 2017.	X	X	
A.6.1.3	Contacto con las autoridades	Se deben tener contactos apropiados con las autoridades pertinentes	SI	Se realiza contacto con la Policía Nacional y la Fiscalía dependiendo del incidente presentado. A4.MS.DE Anexo 4 Manual Políticas de Seguridad de la Información. A6.MS.de Anexo 6. Parte Interesadas	X	X	
A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	SI	Se tiene contacto con la Policía Nacional a través del envío de las NOTICIAS, TIPS Y ALERTAS CSIRT-PONAL. Se participa en la Reunión de Infraestructura Critica, Riesgo operacional y Ciberdefensa. Se participa en talleres con MINTIC	X		
.AB	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	SI	Se cuenta con el A4.MS.DE A4.MS.DE Manual de Políticas de Seguridad de la información. Para usuarios de partes externas se cuenta con la G7.ABS Guía para la Adquisicion de Bienes y Servicios de Calidad desde el proceso de Adquisición de Bienes y Servicios, para los colaboradores se cuenta, desde el proceso de Servicios Administrativos con la G2.SA. Guía Gestión de Bienes y la Resolución No. 9674 del 27 de julio de 2018.	X	X	
A.6.2	**Dispositivos Móviles y teletrabajo**						
A.6.2.1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X	X	X
A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución 7600 del 29 de julio de 2016	x	x	x
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**						
A.7.1	**Antes de asumir el empleo**						
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	SI	La Dirección de Gestión Humana cuenta con un P21.GTH Procedimiento Provision de Empleos y la Dirección de Contratación cuenta con el F2.P5.ABS el Procedimiento para la Solicitud e Inicio del Proceso de Contratación.	X	X	X
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X	X	X
A.7.2	**Durante la ejecución del empleo**						
A.7.2.1	Responsabilidades de la dirección	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	SI	Resolución 7070 de 2017.	X	X	X
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	SI	El ICBF cuenta con un módulo SGSI inmerso en el curso virtual SIGE y con el PL6.GTI Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	X	X	X
A.7.2.3	Proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	Control Interno Disciplinario investiga acciones de los empleados que hayan cometido violación a la seguridad de la información mediante el P2.GTH Procedimiento Proceso Disciplinario Ordinario, de igual manera se cuenta con el P2.RC Procedimiento Quejas Reclamos y Sugerencias	X	X	X
A.7.3	**Terminación y cambio de empleo**						
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X	X	X
A.8	**GESTIÓN DE ACTIVOS**						
A.8.1	**Responsabilidad por los activos**						
A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	El ICBF cuenta con la G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos con orientaciones para el diligenciamiento del formato de activos de información a nivel Nacional.	X	X	X
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	SI	El ICBF debe conocer y clasificar los activos de información.	X	X	X
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI	El ICBF cuenta con A4.MS.DE A4.MS.DE Manual de Políticas de Seguridad de la información, y la Resolución No. 9674 del 27 de julio de 2018	X	X	X

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se entregan a su cargo, al terminar su empleo, contrato o acuerdo.	SI	Se cuenta con el A4.MS.DE A4.MS.DE Manual de Políticas de Seguridad de la información. Para usuarios de partes externas se cuenta con la G7.ABS Guía para la Adquisicion de Bienes y Servicios de Calidad desde el proceso de Adquisición de Bienes y Servicios, para los colaboradores se cuenta, desde el proceso de Servicios Administrativos con la G2.SA. Guía Gestión de Bienes	X	X	X
A.8.2	**Clasificación de la información**						
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada.	SI	La Dirección de Servicio y Atención, y la Oficina de Asesoría Jurídica, revisan el levantamiento de activos para dar cumplimiento a la ley de transparencia 1712 de 2014. Se cuenta con el A4.MS.DE A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X	X	X
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de la información adoptado por la organización.	SI	El ICBF cuenta con la G11.GTI. Guía para la Rotulación de la Información	X	X	X
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Se tiene en cuenta en el levantamiento de activos; su clasificación está basada en la afectación a la triada.	X	X	X
A.8.3	**Manejo de medios**						
A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.	SI	Se cuenta con el P9.GTI Procedimiento para el Manejo de Medios Removibles	X	X	X
A.8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	SI	Se tiene en cuenta el contenido de la G2.SA. Guía Gestión de Bienes mediante la baja de equipos o repotencializar los mismos, teniendo en cuenta que se debe utilizar el IT3.P2.GTI Instructivo para Gestionar Solicitudes de Borrado Seguro de Dispositivos	X	X	X
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	SI	Se cuenta con la G3.SA Guía para la Gestión Documental en el ICBF, asimismo con el P32.SA Procedimiento Transferencias Documentales Primarias y el P31.SA ProcedimientoTransferencias Documentales Secundarias a cargo del proceso de Servicios Administrativos. Se cuenta también con el A4.MS.DE A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X	X	X
A.9	**CONTROL DE ACCESOS**						
A.9.1	**Requisitos del negocio para control de accesos**						
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	SI	Se cuenta con G9.GTI Guía para el control de accesos a centros de cableado y data center, A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información y F1.P2.GTI Formato de Solicitud Servicios de Tecnología	X	X	X
A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI	Se cuenta con el F1.P2.GTI Formato de Solicitud Servicios de Tecnología	X	X	X
A.9.2	**Gestión de acceso de usuarios**						
A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SI	Se cuenta con el F1.P2.GTI Formato de Solicitud Servicios de Tecnología	X	X	X
A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	SI	Se cuenta con el F1.P2.GTI Formato de Solicitud Servicios de Tecnología	X	X	X
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI	Se cuenta con el F1.P2.GTI Formato de Solicitud Servicios de Tecnología	X	X	X
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	SI	Desde el Directorio Activo se establece que se deben cambiar contraseñas en el primer inicio de sesión. Cada 60 días se solicita al usuario cambio de contraseñas. A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información	X	X	X
A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	SI	Desde el Directorio Activo se revisan los derechos de acceso en caso de que haya finalización de contrato, o cambios de rol dentro del ICBF. A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información	X	X	
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	SI	Se cuenta con A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información y el F1.P2.GTI Formato de Solicitud Servicios de Tecnología	X	X	X
A.9.3	**Responsabilidades de los usuarios**						
A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI	La Subdirección de Recursos Tecnológicos capacita y concientiza a los funcionarios y colaboradores regularmente en temas de seguridad de la información, convenientes para realizar sus funciones laborales y actividades. A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información	X	X	X
A.9.4	**Control de acceso a sistemas y aplicaciones**						
A.9.4.1	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	SI	A una cuenta de usuario se le asigna permisos o privilegios para acceder a los sistemas de información y desarrollar actividades dentro de los mismos. Los privilegios delimitan las actividades que el usuario puede desarrollar sobre los sistemas de información. A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información	X		
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	SI	Se hace a través del Directorio Activo, y la política de control de acceso se maneja desde cada aplicativo A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la	X		

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
				Información			
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	SI	Cada 60 días se solicita al usuario cambio de contraseñas. A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información	X		
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	SI	Desde el Directorio activo se asignan privilegios de administrador a las personas que pueden instalar y hacer uso de programas utilitarios. A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información	X		
A.9.4.5	Control de acceso a códigos fuente de programas	Se debe registrar el acceso a los códigos fuente de los programas.	SI	Se cuenta con P6.GTI Procedimiento para desarrollo y mantenimiento de Sistemas de información	X		
A.10	**CRIPTOGRAFIA**						
A.10.1	**Controles criptográficos**						
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	SI	Se cuenta con el A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información y la Resolución No. 9674 del 27 de julio de 2018	X		
A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante su ciclo de vida.	SI	Para la transferencia electrónica se tienen en cuenta aspectos de seguridad sobre la información y realización de pagos del ICBF. G1.P17.GF Guía de Políticas y Seguridad para el Manejo y Control de los Recursos Financieros Administrados por el ICBF A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la	X		
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**						
A.11.1	**Áreas seguras**						
A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X	X	X
A.11.1.2	Control de accesos físicos	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite acceso a personal autorizado.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X	X	X
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X	X	X
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y el P29.SA Procedimiento Gestión Ambiental Administrativa.	X	X	X
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información	X	X	X
A.11.1.6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información	X	X	
A.11.2	**Equipos**						
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información	X	X	X
A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información	X	X	X
A.11.2.3	Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X	X	X
A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	Existen actas de mantenimiento de equipos realizados por los ingenieros regionales y la UT.	X	X	X
A.11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información y con la minuta de vigilancia para la salida de los equipos.	X	X	X
A.11.2.6	Seguridad de activos y equipos fuera de la oficina	Se deben aplicar medidas de seguridad a los activos que se encuentran instalaciones fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información.	X		
A.11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	SI	Desde el proceso de Servicios Administrativos se cuenta con una G2.SA Guia Gestion de Bienes	X		
A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información.	X	X	X
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información.	X	X	X
A.12	**SEGURIDAD DE LAS OPERACIONES**						
A.12.1	**Procedimientos operacionales y responsabilidades**						
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	SI	Se encuentra publicado en la Intranet todos los procedimientos operativos de cada proceso del ICBF.	X	X	X
A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI	Se cuenta con el P4.GTI Procedimiento de Gestión De Cambios De Tecnologías De La Información.	X		
A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	SI	Se cuenta con el A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información y con un PL1.GTI Plan de Capacidad.	X		
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	Se deben separar los ambientes de desarrollo ,prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	SI	Se cuenta con el A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información.	X		
A.12.2	**Protección contra códigos maliciosos**						

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.12.2.1	Controles contra códigos maliciosos	Se deben implementar controles de detección, de prevención y de recuperación combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos.	SI	Se contrató Servicio de SOC con el nuevo proveedor de servicios. Se cuenta con A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	X
A.12.3	**Proteger contra la perdida de datos**						
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI	Se cuenta con procedimientos, guías e instructivos referentes al respaldo y restauración de información G8.GTI Guía De Respaldo Y Restauración De Copias De Seguridad	X	X	X
A.12.4	**Registro y seguimiento**						
A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros a cerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	SI	Se tiene Servicio de SOC contratado con el proveedor de servicios. P11.GTI Procedimiento De Gestion De Eventos Y Alertas	X		
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado	SI	Se tiene Servicio de SOC contratado con el proveedor de servicios. P11.GTI Procedimiento De Gestion De Eventos Y Alertas	X		
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	SI	Se tiene Servicio de SOC contratado con el proveedor de servicios. P11.GTI Procedimiento De Gestion De Eventos Y Alertas	X		
A.12.4.4	Sincronización de reloj	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	SI	Se cuenta con A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información.	X		
A.12.5	**Control de software operacional**						
A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	Se cuenta con A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información.	X		
A.12.6	**Gestión de la vulnerabilidad técnica**						
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	SI	Se elabora y ejecuta Test de Penetración, y se elabora Informe de resultados. Se cuenta con P1.GTI Procedimiento Seguimiento, Control Y Atención De Vulnerabilidades Técnicasde igual manera se cuenta con el A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información.	X		
A.12.6.2	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	SI	Se cuenta con el A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	X
A.12.7	**Consideraciones sobre auditorías de sistemas de información**						
A.12.7.1	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI	Se cuenta con el A4.MS.DE Anexo 4 Manual de Políticas de Seguridad de la Información.	X		
A.13	**SEGURIDAD DE LAS COMUNICACIONES**						
A.13.1	**Gestión de la seguridad de las redes**						
A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	Se cuenta con plataforma tecnológica para soportar los sistemas.	X	X	
A.13.1.2	Seguridad de los servicios de red	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI	Se cuenta con informes mensuales de los servicios firewall, WAN y LAN realizados por los proveedores.	X X		
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI	Se cuenta con segmentación de redes en el ICBF.	X	X	
A.13.2	**Transferencia de información**						
A.13.2.1	Políticas y procedimientos de transferencia de información	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información.	X	X	X
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	SI	Se cuenta con acuerdos de confidencialidad para la transferencia de información entre el ICBF y los proveedores (Información recopilada de los repositorios del ICBF, los cuales requieren permisos de acceso).	X		
A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	Se cuenta con correo electrónico institucional Exchange.	X		
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	SI	Desde la Dirección de Contratación a través de las minutas de los contratos de prestación de servicios se incluye una cláusula de confidencialidad. adicionalmente se cuenta con la una G7.ABS Guía para la Adquisicion de Bienes y Servicios de Calidad en donde se contempla una obligación del eje de seguridad de la información referente a establecer acuerdos de confidencialidad con los proveedores.	X	X	X
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**						
A.14.1	**Requisitos de seguridad de los sistemas de información**						
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI	La Subdirección de Sistemas Integrados de Información cuenta con el P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información	X	X	X
A.14.1.2	Seguridad de servicio de las aplicaciones en redes publicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI	La Subdirección de Sistemas Integrados de Información cuenta con el P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información	X		
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado la alteración no autorizada de mensajes, la divulgación no autorizada y la divulgación o reproducción de mensajes no autorizados.	SI	La Subdirección de Sistemas Integrados de Información cuenta con el P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información	X		
A.14.2	**Seguridad en los procesos de desarrollo y soporte**						
A.14.2.1	Políticas de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información.	X		

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.14.2.2	Procedimiento de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	SI	Se cuenta con un Procedimiento P4.GTI Gestión de Cambios de Tecnologías de la Información y P3.GTI Procedimiento Gestión Cambios Emergencia Tecnologías de Información	X		
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	SI	Se cuenta con un Procedimiento P4.GTI Gestión de Cambios de Tecnologías de la Información y P3.GTI Procedimiento Gestión Cambios Emergencia Tecnologías de Información	X		
A.14.2.4	Restricción en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI	Se cuenta con un Procedimiento P4.GTI Gestión de Cambios de Tecnologías de la Información y P3.GTI Procedimiento Gestión Cambios Emergencia Tecnologías de Información	X		
A.14.2.5	Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros , y aplicarlos a cualquier actividad de implementación de sistemas de información.	SI	Se cuenta con la G1.GTI Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información	X		
A.14.2.6	Ambiente seguro de desarrollo	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas .	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información.	X		
A.14.2.7	Desarrollo externamente contratado	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	Se obliga al cumplimiento a través de las cláusulas de los contratos asociados al desarrollo de software	X		
A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	SI	Se cuenta con el P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información donde se incluyen pruebas de funcionalidad	X		
A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados .	SI	Se cuenta con el P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información donde se incluyen pruebas de funcionalidad	X		
A.14.3	**Datos de pruebas**						
A.14.3.1	Protección de datos de pruebas	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información.	X		
A.15	**RELACIONES CON LOS PROVEEDORES**						
A.15.1	**Seguridad de la información en las relaciones con los proveedores**						
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	SI	Se cuenta con la Resolución No. 9674 del 27 de julio de 2018 y Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información	X		
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	SI	Se cuenta con la Resolución No. 9674 del 27 de julio de 2018 y Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información	X		
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información	X		
A.15.2	**Gestión de la prestación de servicios de proveedores**						
A.15.2.1	Seguimiento y revisión a los servicios proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información	X		
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	SI	Se cuenta con el A4.MS.DE Manual de Políticas de Seguridad de la información	X		
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**						
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**						
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	Se cuenta con el P5 GTI Procedimiento gestión de incidentes de seguridad de la información, con el A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018	X		
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	SI	Se cuenta con el P5 GTI Procedimiento gestión de incidentes de seguridad de la información y el A4.MS.DE Manual de Políticas de Seguridad de la información.	X	X	X
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	SI	Se cuenta con el P5 GTI Procedimiento gestión de incidentes de seguridad de la información y el A4.MS.DE Manual de Políticas de Seguridad de la información.	X	X	X
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decir si se van a clasificar como incidentes de seguridad de la información.	SI	Se cuenta con el P5 GTI Procedimiento gestión de incidentes de seguridad de la información y con el A4.MS.DE Manual de Políticas de Seguridad de la información	X		
A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI	Se cuenta con el P5 GTI Procedimiento gestión de incidentes de seguridad de la información y el A4.MS.DE Manual de Políticas de Seguridad de la información.	X		
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	SI	Se hace a través de la Base de Datos de Conocimiento. Alojada en la herramienta de gestión de mesa de servicio.	X		
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que puede servir como evidencia.	SI	G5.GTI Guía de Recolección de Evidencias de Elementos Informáticos	X		
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**						
A.17.1	**Continuidad de seguridad de la información**						
	Planificación de la continuidad de la seguridad	La organización debe determinar sus requisitos para la seguridad de la y la continuidad de la gestión de la		Se cuenta con la Resolución 7070 de 2017, el A4.MS.DE Manual de Políticas de Seguridad de la información y con el PL3.GTI Plan			

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.17.1.1	de la información	seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	SI	de Continuidad del Negocio.	X	X	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	SI	Se cuenta con la Resolución 7070 de 2017, el A4.MS.DE Manual de Políticas de Seguridad de la información y con el PL3.GTI Plan de Continuidad del Negocio.	X	X	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados , con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	SI	Se cuenta con la Resolución 7070 de 2017, el A4.MS.DE Manual de Políticas de Seguridad de la información y con el PL3.GTI Plan de Continuidad del Negocio.	X	X	
A.17.2	**Redundancia**						
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	Se cuenta con la Resolución 7070 de 2017, el A4.MS.DE Manual de Políticas de Seguridad de la información y con el PL3.GTI Plan de Continuidad del Negocio.	X		
A.18	**CUMPLIMIENTO**						
A.18.1	**Cumplimiento de requisitos legales y contractuales**						
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.	SI	Se cuenta con la Matriz de verificación de Requisitos Legales y el P4.MI Procedimiento Identificación y Evaluación de Requisitos Legales, para asegurar que se identifique y verifique el cumplimiento de los requisitos legales.	X	X	X
A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos , de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	SI	Se cuenta con el servicio de licenciamiento de software; se cuenta con documento preliminar de política Antipiratería Instituto Colombiano de Bienestar Familiar; Se cuenta con una serie de obras y software registrado MINISTERIO DEL INTERIOR DIRECCIÓN NACIONAL DE DERECHO DE AUTOR, de igual manera se encuentran registradas algunas marcas ante la SuperIntendencia de Industria y Comercio - SIC	X	X	X
A.18.1.3	Protección de registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	SI	La Dirección Administrativa a través del grupo de Gestión Documental establece directrices de retención de registros e información.	X	X	X
A.18.1.4	Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI	Se cuenta con: la Política de Protección de datos personales, el P12.GTI Procedimiento Interno de Registro de Bases Datos Personalescon y su anexo al registro inicial de las bases de datos de datos, el P15.GTI Procedimiento para la actualizacion, revocacion y supresion de datos personales y el P14.GTI Procedimiento Intercambio o Suministro de Informacion	X	X	X
A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	SI	Se cuenta con Controles Criptográficos identificados	X		
A.18.2	**Revisiones de seguridad de la información**						
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	SI	Se cuentan con el P2.EI Procedimiento Auditorias Internas SIGE y la formulación del plan de auditorias.	X	X	X
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas , y cualquier otro requisito de seguridad.	SI	A través del PL6.GTI Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, se divulgan las Políticas de Seguridad de la Información contenidas en el A4.MS.DE A4.MS.DE Manual de Políticas de Seguridad de la información y la Resolución No. 9674 del 27 de julio de 2018. De igual manera se han identificado oportunidades de mejora y acciones correctivas por el incumplimiento de las políticas de seguridad de la información.	X	X	X
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI	Se cuenta con el P1.GTI Procedimiento Seguimiento Control y Atención de Vulnerabilidades Técnicas y su F1.P1.GTI Formato de Registro de Pruebas y Remediacion Vulnerabilidades, asimismo una G14.GTI Guía Desarrollo Pruebas Penetración.	X		